



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/555,929	06/06/2000	IAN R FAIRMAN	36-1334	9644

7590 12/22/2003  
NIXON & VANDERHYE  
1100 NORTH GLEBE ROAD  
8TH FLOOR  
ARLINGTON, VA 22201-4714

EXAMINER

HA, LEYNNA A

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 12/22/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/555,929

Applicant(s)

FAIRMAN ET AL.

Examiner

LEYNNA T. HA

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☐ Responsive to communication(s) filed on \_\_\_\_.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-28 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-28 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. §§ 119 and 120**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☒ Some \* c) ☐ None of:  
1. ☒ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
\* See the attached detailed Office action for a list of the certified copies not received.
- 13) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.  
a) ☐ The translation of the foreign language provisional application has been received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892) 4) ☐ Interview Summary (PTO-413) Paper No(s). \_\_\_\_
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 3. 6) ☐ Other: .

**DETAILED ACTION**

1. Claims 1-28 have been examined and is rejected under 35 U.S.C. 102(e).
2. Claim 27 is objected for minor informalities.

**Claim Rejections - 35 USC § 102**

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

3. ***Claims 1-28 are rejected under 35 U.S.C. 102(e) as being anticipated by Ming, Et Al. (US 5,710,815).***

**As per claim 1:**

Ming, Et Al. teaches a method of distributing digitally encoded data, comprising:

- a) dividing said data into a multiplicity of frames, **(col.4, lines 3-4)**
- b) encrypting said frames, **(col.14, lines 13-22)**
- c) distributing multiple copies of the said data frames to multiplicity of users, **(col.17, lines 35-45)**
- d) communicating a seed value for key generation to respective secure modules located at each of the multiplicity of users, **(col.14, lines 41-66)**
- e) decoding the data frames at respective users using keys derived from the seed value communicated to the secure module, **(col.15, lines 11-13)**
- f) passing a control message to the secure module at a selected one or more of the multiplicity of users, **(col.14, lines 45-48 and col.17, lines 5-15)**
- g) at the or each of selected user, in response to the said control message, controlling the availability of keys generated from the said seed value, thereby controlling access by the users to the said data. **(col.17, lines 35-46)**

**As per claim 2:**

Ming discloses a control field is distributed to each of the multiplicity of users, and the secure module is arranged to enable decryption of a respective frame only when the said control field has been passed to the secure module.

**(col.23, lines 43-65)**

**As per claim 3:**

Ming discloses a control message for modifying the availability of keys is communicated to the secure module in the said control field. **(col.10, lines 45-53)**

**As per claim 4:**

Ming discloses each data frame includes a frame identity field, and each key generated by the secure module is specified to one frame identified by the said field. **(col.11, lines 7-15 and col.11, lines 43-66)**

**As per claim 5:**

Ming discloses the step of distributing multiple copies of the said data comprises multicasting packets of data via a communications network to the plurality of users. **(col.6, lines 6-16)**

**As per claim 6:**

Ming discloses a control message is distributed with a data frame to the multiplicity of users, a user identity field identifying a selected user or group of users is included in the control message, and the control message is acted on only by the user or group of users identified by the said user identity field. **(col.11, lines 7-44)**

**As per claim 7:**

Ming discloses a control message includes a stop flag, and in response to the stop flag the generation of keys at the or each selected user is stopped. **(col.21, lines 43-56)**

**As per claim 8:**

Ming discusses returning a response signal from the secure module to the source of the control message. **(col.18, lines 1-9)**

**As per claim 9:**

Ming discloses a control message includes a contact sender flag, and the step of returning a response signal from the secure module is carried out when the contact sender flag is set. **(col.27, lines 46-55)**

**As per claim 10:**

Ming discusses transmitting a further control message to the user on receipt of the said response signal. **(col.18, lines 25-35)**

**As per claim 11:**

Ming teaches a method of operating a customer terminal in a data communications system, the method comprising:

- a) receiving at the customer terminal a multiplicity of encrypted data frames **(col.14, lines 13-22)**
- b) receiving at the customer terminal a seed value for key generation
- c) passing said seed value for key generation to a secure module located at the customer terminal, **(col.14, lines 41-66)**
- d) generating in the secure module using the seed value keys for decryption of data frames; **(col.15, lines 11-13)**
- e) decrypting the data frames using keys; **(col.23, lines 45-65)**

f) passing to the said secure module a control message received from a source remote from the customer terminal, **(col.15, lines 40-48)**

g) in response to the said control message controlling the availability of keys generated from the said seed value, thereby controlling access by the users to the said data. **(col.17, lines 35-46)**

**As per claim 12:**

Ming teaches a method data communications system comprising:

a) a remote data source arranged to output a plurality of frames, **(col.14, lines 44-65)**

b) encryption means for encrypting the plurality of frames with different respective keys, **(col.14, lines 13-22)**

c) communications channel arranged to distribute multiple copies of the encrypted data frames, **(col.15, lines 22-44)**

d) multiplicity of customer terminals arranged to receive from the communications channel respective copies of the encrypted data frames, **(col.5, lines 55-67)**

e) a key generator located at a customer terminal and programmed to generate from a seed value keys for use in decrypting data frames: **(col.15, lines 11-13)**

f) a key control means connected to the key generator, the key control means comprising:

an interface for receiving control messages; and **(col.18, lines 1-9)**

control means responsive to the said control messages and arranged to control the availability to the user of keys generated from the seed value; and  
**(col.17, lines 33-45)**

g) decryption means connected to the key generator and arranged to decrypt the data frames received at the customer terminal from the communications channel. **(col.23, lines 45-63)**

**As per claim 13:**

Ming discusses the communications channel is a packet-switched data network. **(col.7, lines 3-10)**

**As per claim 14:**

Ming teaches a customer terminal for use in a method according to any one of claims 1 to 11, the customer terminal comprising:

a) a data interface for connection to a data communications channel;  
**(col.18, lines 1-9)**

b) a key generator programmed to generate from a seed value keys for use in decrypting data frames: **(col.15, lines 11-13)**

c) a key control means connected to the key generator, the key control means comprising:

an interface for receiving control messages; and **(col.18, lines 1-9)**

control means responsive to the said control messages and arranged to control the availability to the user of keys generated from the seed value; and  
**(col.17, lines 33-45)**



d) decryption means connected to the key generator and arranged to decrypt the data frames received at the customer terminal from the communications channel. **(col.23, lines 45-63)**

**As per claim 15:**

Ming teaches a data server for use in a method according to any one of claims 1 to 10, the data server comprising:

a) a data interface for connection to a data communications channel;

**(col.18, lines 1-9)**

b) means for outputting encrypted data frames via the data interface onto the communications channel for receipt by a multiplicity of customer terminals; **(col.14, lines 44-65)**

c) means for outputting control messages onto a data communications channel for controlling the operation of key generators at customer terminals.

**(col.19, lines 2-19)**

**As per claim 16:**

Ming discusses generating keys from the seed value by iterated operations on a seed value by selected ones of a plurality of predetermined functions.

**(col.15, lines 22-25)**

**As per claim 17:**

Ming discusses a method of decrypting data frames characterized by generating a decryption key from the seed value by iterated operations on a seed value by selected ones of a plurality of predetermined functions. **(col.15, lines 10-12)**

**As per claim 18:**

Ming discusses the selection of the said predetermined functions is determined by the value of a frame identity number. **(col.19, lines 21-50)**

**As per claim 19:**

Ming discusses the predetermined functions are computationally symmetric. **(col.17, lines 35-50)**

**As per claim 20:**

Ming discusses the said functions are left-shifted binary XOR and right-shifted binary XOR. **(col.16, lines 22-24)**

**As per claim 21:**

Ming discloses applying different characteristic variations to data decrypted at different respective customer terminals. **(col.16, lines 25-30)**

**As per claim 22:**

Ming discusses the plurality of remote data sources, each outputting a respective plurality of frames. **(col.17, lines 17-22)**

**As per claim 23:**

Ming discusses the customer terminal receives a primary seed value common to different respective data streams from the plurality of data sources **(col.14, lines 41-46)**, and derives from the common primary key a plurality of different respective secondary seed values for decrypting frames from different respective data sources. **(col.14, lines 47-67)**

**As per claim 24:**

Ming discusses the data received from different data sources includes different respective source identity values, **(col.17, lines 16-42)** and the respective secondary seed value is generated from the primary seed value by modifying the primary seed value with the source identity value. **(col.14, lines 41-67)**

**As per claim 25:**

Ming discloses each data frame includes a frame type field. **(col.17, lines 46-55)**

**As per claim 26:**

Ming teaches a method for storing a receipt including data from the frame type field. **(col.11, lines 7-15)**

**As per claim 27:**

Ming teaches a method of distributing digitally encoded data, comprising:

- a) dividing said data into a multiplicity of frames, **(col.4, lines 3-4)**
- b) encrypting said frames, **(col.14, lines 13-22)**
- c) marking frames with a frame type field **(col.15, lines 15-29)**
- d) communicating said data frames to a user, **(col.19, lines 4-9)**
- e) communicating a seed value for key generation to the user **(col.14, lines 41-45)**
- f) decoding the data frames at the users using keys derived from the seed value **(col.15, lines 11-13)**

Art Unit: 2131

g) generating and storing receipts for said data frames, said frames including the frame type data from the frame type field. **(col.23, line 54 thru col.24, line 2)**

**As per claim 28:**

Ming teaches communicating receipts to a third party, and obtaining from the said third party a payment for receipt of data of a specified type. **(col.27, lines 3-63)**

**Claim Objections**

**4. Claim 26 is objected to because of the following informalities:** On lines 5-9, the letters “d), d), e), f)” are not consecutive and should be “d), e), f), g).  
**Appropriate correction is required.**

**Conclusion**

***For more details and information of the cited rejections above, please refer to:***

Ming, Et Al. (US 5,710,815): col.2, line 11...ET. Seq.

***5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.***


Salomaki (US 6,222,924): col.2, line 44...ET. Seq.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (703) 305-3853. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ SHEIKH can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 746-7239.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 306-5631.

LHa

  
GILBERTO BARRON  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100